

Describe in writing 5 different commands used in Windows :

Ipconfig: Displays current Ip address both [IPv6 and IPv4], Subnet Mask and Default gateway.

Hostname: Displays the current name of the workstation or Server.

Cd [location or .. or /]: Short for change directory, this command will set your active directory to the destination file if specifically named or if .. or / is used will move you up one directory level.

Dir: Displays the contents of Current Directory

Getmac: Displays the Mac Address of the system.

Describe in writing what are viruses and malware discussed in Module 2

The WannaCry Worm was Ransomware that affected over 300,000 systems that would encrypt all the files on a system and show a message asking for ransom to be sent to someone. It was officially attributed to North Korea in 2017 by the US. WannaCry was stopped by Marcus Hutchins accidentally just a few short days after it was discovered.

The Mirai Malware is a Linux base malware first found in August 2016 that would turn any network device running Linux into a bot for a botnet. It primarily targeted internet cameras and home routers. A botnet is a group of internet connected devices that are usually controlled by an individual usually used to perform DDoS attacks on websites or servers to make them inoperable. That is what the Mirai Botnet did, they use this botnet to take down many popular sites such as Minecraft and was also used to attack a French web host called OVH. This Malware was created by Paras Jha, Josiah White and Dalton Norman and there are still variants of this malware out there today!

“Triple Threat” also known as triple extortion. “Triple Threat” refers to the evolution of cyber threats and the fact that threat actors are starting to stack different cyber-attacks into one attack. They would do this by first infecting the target with ransomware and demanding payment. They would then also inform the target that they have exfiltrated sensitive data and that if they don’t pay a second ransom, they would release the data and harm their reputation. After a short time when the target thinks they’re safe, they would then attack the same target a third time usually with a distributed denial-of-service attack to disrupt business operations and would follow up with another ransom demand to stop the attacks.

Describe in writing what are the best practices to prevent viruses and malware

The best practices are as follows:

1. Have Windows Defender Installed and up to date and Active.
2. Don't open any file in an email unless you can verify that the person that sent it is legitimate.
3. Keep Windows and all applications on the system or server Up to date.
4. Don't click on unverified links in emails.
5. Perform regular backups.

Describe in writing what are local users and groups in Server (What are each used for?)

Local users on a server allows for multiple individuals to work on a single server without the need to share account and passwords. It also allows for control and logging of what individuals are doing on the server. It also allows individuals to work on the server with less permissions than the administrator.

Groups on a server enable the ability to group users into having access to resources that they need to have access to. It gives us the ability to control access to resources and ensure only people who have a need can access certain resources. It also enables us to give and remove access more easily than changing the access permissions on 50 folders you only need to add or remove users in one place.

Describe in writing what are permissions in Server

Permissions are rules that say what actions users or groups can perform to files, folders, printers, or permissions and settings.

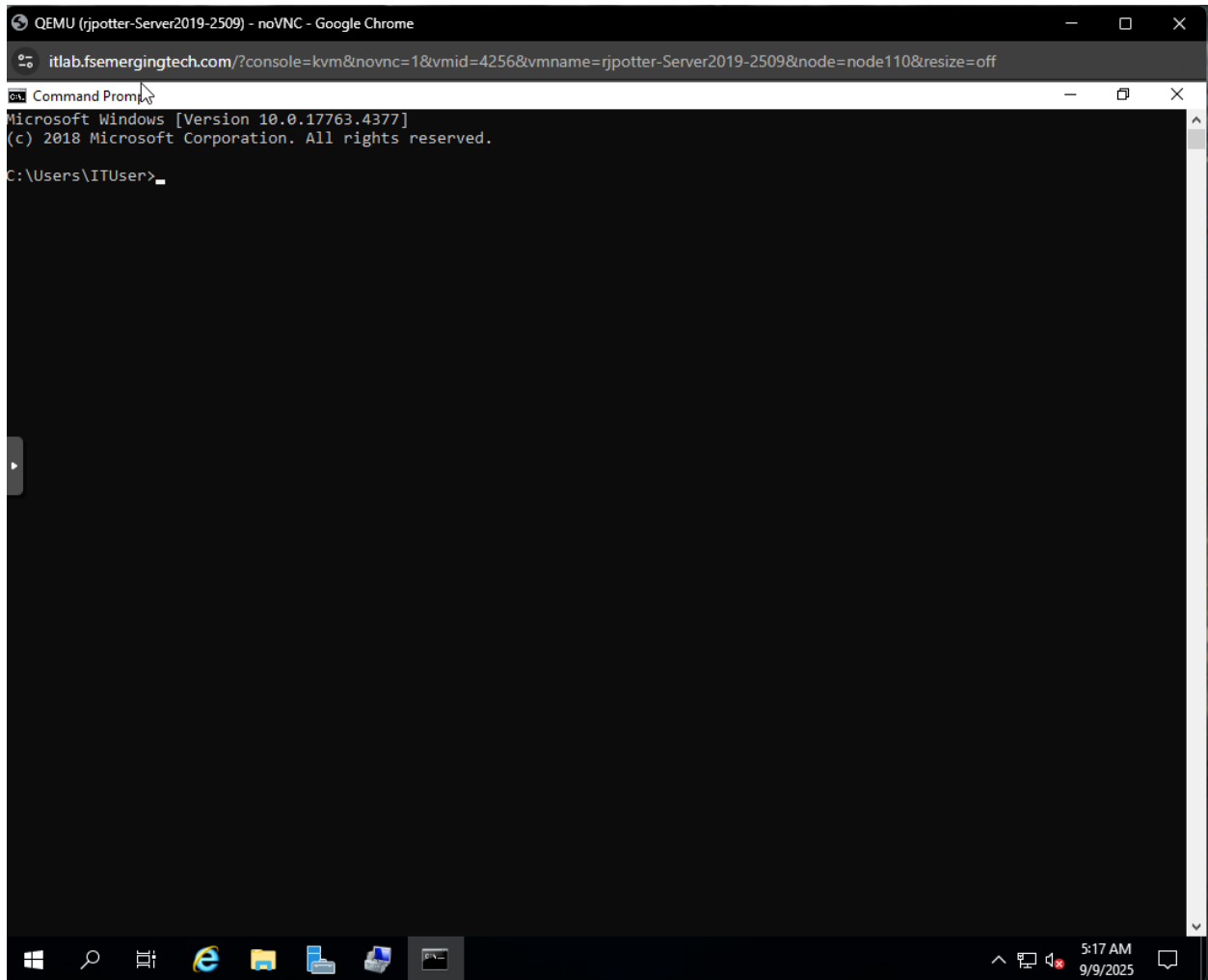
Describe in writing how to change permissions in Server

For File Permissions Right click on the Folder you wish to change permissions for > Select Properties > Select the "Security" Tab > Click Edit > Here you can Click Add to add new users or Click on an existing User from the list and Edit and apply new permissions for them.

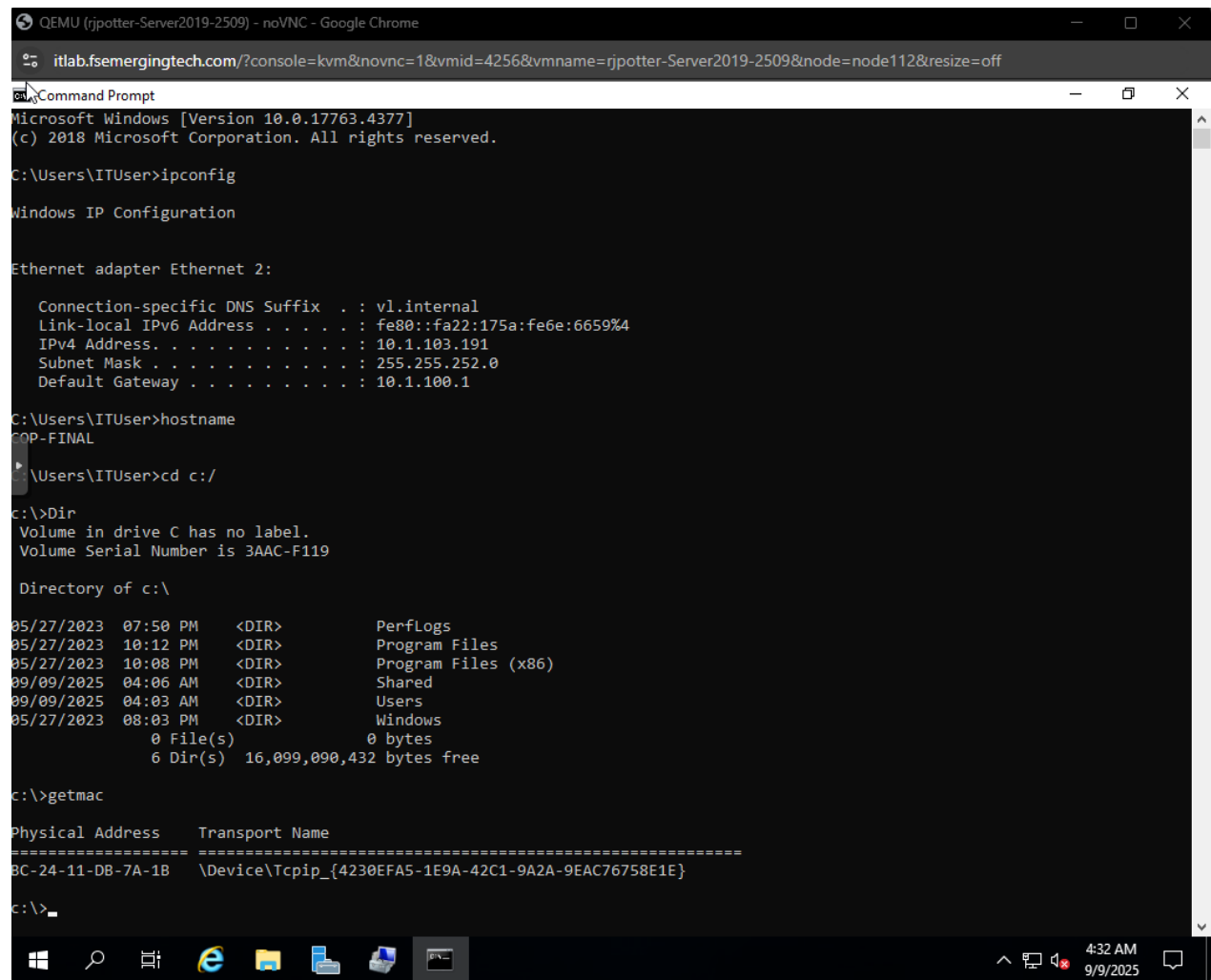
Describe in writing what is the command prompt in Windows workstation/Server

Command Prompt is a text-based interface for windows. It allows an administrator to run command to perform administrative tasks, manage files, troubleshoot issues, and configure system files in a very efficient way.

Screenshot using the command prompt in Windows workstation or Server



Execute some of the commands you explained in Question 1 above



```
QEMU (rjpotter-Server2019-2509) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=4256&vmname=rjpotter-Server2019-2509&node=node112&resize=off

Command Prompt
Microsoft Windows [Version 10.0.17763.4377]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ITUser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : vl.internal
    Link-local IPv6 Address . . . . . : fe80::fa22:175a:fe6e:6659%4
    IPv4 Address. . . . . : 10.1.103.191
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 10.1.100.1

C:\Users\ITUser>hostname
COP-FINAL

C:\Users\ITUser>cd c:/

c:\>Dir
Volume in drive C has no label.
Volume Serial Number is 3AAC-F119

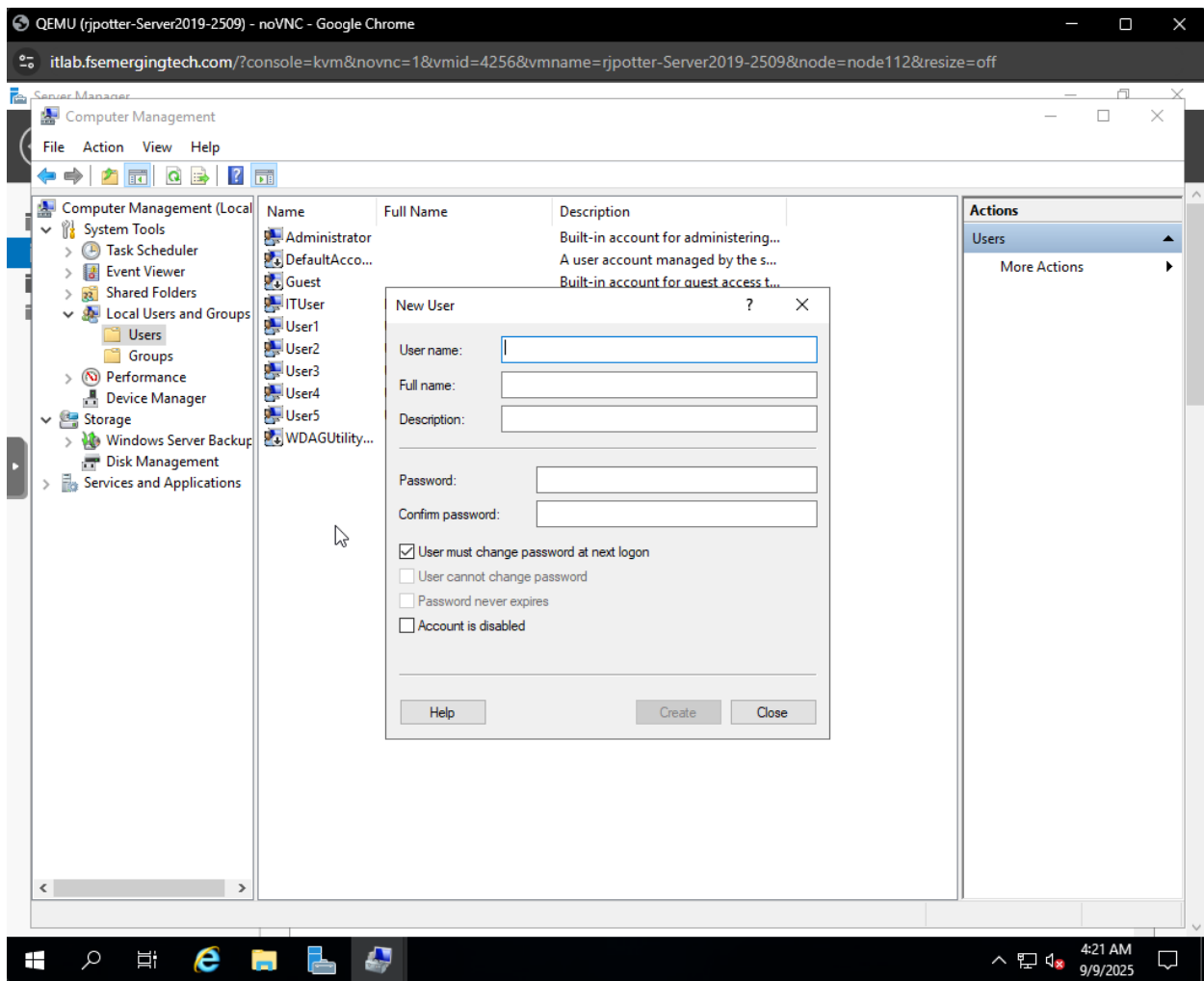
Directory of c:\

05/27/2023  07:50 PM    <DIR>          PerfLogs
05/27/2023  10:12 PM    <DIR>          Program Files
05/27/2023  10:08 PM    <DIR>          Program Files (x86)
09/09/2025  04:06 AM    <DIR>          Shared
09/09/2025  04:03 AM    <DIR>          Users
05/27/2023  08:03 PM    <DIR>          Windows
               0 File(s)                0 bytes
               6 Dir(s)  16,099,090,432 bytes free

c:\>getmac

Physical Address      Transport Name
=====
8C-24-11-DB-7A-18    \Device\NPF{4230EFA5-1E9A-42C1-9A2A-9EAC76758E1E}
```

Screenshot how to create a local user in Windows workstation or Server



Screenshot the User directory in the C: drive in Server where the local user accounts were created when completing module 2.5

